

IN THE CLAIMS:

Please cancel claims 1 – 26 in their entirety and without prejudice and substitute the following new claims:

1 --27. A method for protecting one or more computer systems using the
2 same secret key (Ks) cryptographic algorithm, characterized in that secret data (Ds)
3 stored in a secret area of the computer system or systems is utilized to perform a
4 cryptographic calculation for each computer system and for each secret key.

1 28. The method according to claim 27, characterized in that, for each
2 computer system and for each secret key (Ks), the way in which said secret data
3 (Ds) is used to perform said cryptographic calculation is public.

1 29. The method according to claim 27, characterized in that in each of the
2 computer systems, each secret key (Ks) used by said cryptographic calculation
3 corresponds to a specific piece of said secret data (Ds).

1 30. A method according to claim 27 for protecting one or more computer
2 systems wherein the cryptographic calculation uses nonlinear transformations of km
3 bits into kn bits described by k conversion tables in which n output bits of the
4 transformation are read at an address that is a function of the km input bits, and for
5 each of said nonlinear transformations, said k tables are part of the secret data (Ds).

1 31. A method according to claim 27 for protecting one or more computer
2 systems wherein the cryptographic calculation process uses nonlinear
3 transformations of km bits into kn bits described by k conversion tables in which n
4 output bits of the transformation are read at an address obtained by applying a
5 secret bijective function (ϕ) to an m-bit value, itself obtained by applying a public
6 function of the km input bits of the nonlinear transformation, and for each of said
7 nonlinear transformations, said k tables are part of the secret data (Ds).

1 32. The method according to claim 27, comprising storing a conversion table
2 calculation program in each computer system and activating the calculation program
3 by a given event in order to calculate tables and store all or part of said tables in the
4 secret data (Ds)..

1 33. A computer system comprising storage means for storing a modified
2 cryptographic algorithm that adheres to computational phases of a standard
3 cryptographic algorithm, a secret encryption key contained in a secret area of the
4 storage means for modifying the standard cryptographic algorithm, means for
5 executing said modified cryptographic algorithm, first secret means for replacing
6 intermediate variables required for the computational phases of the standard
7 algorithm with a plurality (k) of partial intermediate variables, second means for
8 applying a nonlinear transformation table to each of said partial intermediate
9 variables, and third secret means for reconstituting a final result corresponding to
10 utilization of the standard cryptographic algorithm from results obtained on the partial
11 variables.

1 34. A computer system according to claim 33, characterized in that secret
2 encryption key stored in the secret area includes at least one first random variable v_1
3 constituting at least one secret partial variable, and the modified cryptographic
4 algorithm determines at least one other partial variable v_2 , by applying a first secret
5 function to the intermediate variable v and the secret partial variable or variables v_1 .

1 35. A computer system according to claim 34, characterized in that the
2 modified cryptographic algorithm includes tables used for applying the nonlinear
3 transformations to the partial variables v_1 and v_2 , at least one of said tables (A),
4 formed by random selection, and being stored in the secret data Ds, the other tables
5 required for the calculations being stored in a nonvolatile memory, means for
6 executing various computational rounds of the standard algorithm, each time using
7 the tables on the partial variables, and means for calculating the result in the last
8 round of the algorithm by combining the partial variables in accordance with a
9 second secret function.

1 36. A computer system according to claim 33, characterized in that the first
 2 secret means of the modified algorithm are constituted by a function f , linking the
 3 partial intermediate variables and each intermediate variable (v), such that the
 4 knowledge of one value of said intermediate variable never makes it possible to
 5 deduce all of the particular partial values v_i such that there exists a $(k-1)$ -tuple $(v_1,$
 6 $\dots, v_{i-1}, v_{i+1}, \dots, v_k)$ that satisfies the equation $f(v_1, \dots, v_i, \dots, v_k) = v$.

1 37. A computer system according to claim 33, characterized in that the
 2 second means of the modified algorithm are constituted by k partial conversion
 3 tables, and among the k partial conversion tables, $k-1$ partial conversion tables
 4 contain secret random variables.

1 38. A computer system according to claim 37, characterized in that the
 2 second means of the modified algorithm comprise k conversion tables, each of said
 3 conversion tables receiving an input a value obtained by applying a secret bijective
 4 function ϕ_j to said function $f(v_1, \dots, v_k)$ of the partial intermediate variables in
 5 accordance with the relation $\phi_j \circ f(v_1, \dots, v_k)$, $j \in [1, k]$, this application $\phi_j \circ f(v_1, \dots, v_k)$
 6 being performed by direct evaluation of a resulting value, this resulting value, applied
 7 to the input of the conversion table, making it possible to read n output bits of the
 8 transformation at an address that is a function of these m input bits.

1 39. A computer system according to claim 33, characterized in that the
 2 second means of the modified algorithm comprise means for replacing each
 3 nonlinear transformation applied to an intermediate variable of the standard
 4 cryptographic calculation process, without a separation, with a partial nonlinear
 5 transformation of km bits into kn bits applied to all of the partial intermediate
 6 variables, means for calculating $(k-n)$ of said output bits of this transformation as a
 7 polynomial function of the km input bits, and means for reading the remaining n bits
 8 of said output bits by reading a conversion table in which the n remaining bits are
 9 read at an address that is a function of the km input bits.

1 40. A computer system according to claim 33, characterized in that it

2 further includes means for sequentially executing operations performed by the
 3 modified algorithm in the various parts resulting from the separation of the
 4 cryptographic calculation process into several distinct calculation process parts.

1 41. A computer system according to claim 33, characterized in that it includes
 2 means for executing, in interleaved fashion, operations performed in the various
 3 parts resulting from the separation of the cryptographic calculation process into
 4 several distinct calculation process parts.

1 42. A computer system according to claim 33, characterized in that it includes
 2 means for simultaneously executing operations performed in the various parts
 3 resulting from the separation of the cryptographic calculation process into several
 4 distinct calculation process parts, in the event of multiprogramming.

1 43. A computer system according to claim 33, characterized in that it includes
 2 means for simultaneously executing, in different processors working in parallel, the
 3 operations performed in the various parts resulting from the separation of the
 4 cryptographic calculation process into several distinct calculation process parts.

1 44. A computer system according to claim 33, characterized in that it includes
 2 a conversion table calculation program stored in each computer system and means
 3 for activation by a given event of the calculation of the tables and for the storage of
 4 all or part of these tables in the secret data.

1 45. A computer system according to claim 33, further including a counter
 2 having means for storing a value that is incremented with each cryptographic
 3 calculation so as to constitute a given event for the activation, by activating means,
 4 of the calculation of the tables when a given value is exceeded.--